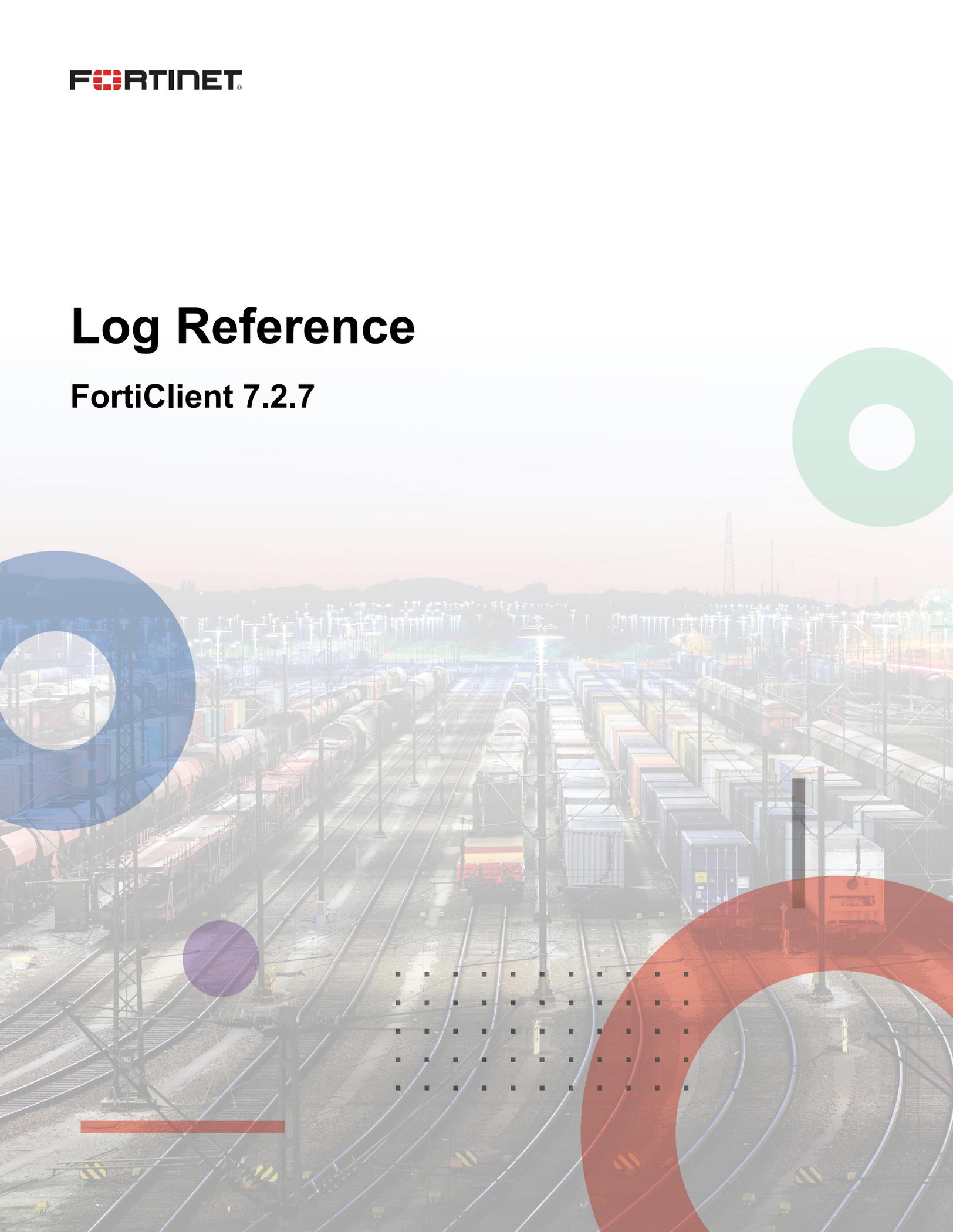


Log Reference

FortiClient 7.2.7



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



December 12, 2024

FortiClient 7.2.7 Log Reference

04-727-877833-20241212

TABLE OF CONTENTS

Change log	4
Introduction	5
Windows	6
Mandatory fields	6
Log fields by type	7
securityevent	7
systemevent	9
Log message by type	10
securityevent > av	10
securityevent > vulnerabilityscan	11
systemevent > endpoint	12
Linux	15
Mandatory fields	15
Log fields by type	16
securityevent	16
systemevent	18
Log message by type	19
securityevent > av	19
securityevent > vulnerabilityscan	20
systemevent > endpoint	21

Change log

Date	Change description
2024-12-12	Initial release.

Introduction

This document provides information about all the log messages applicable to FortiClient 7.2.7. The logs are intended for administrators to use as reference for more information about a specific log entry and message that FortiClient generated.

FortiClient has the following log types:

- Security event
- System event
- Traffic

This document contains the following information:

- [Windows on page 6](#): fields that apply to FortiClient (Windows) logs
- [Linux on page 15](#): fields that apply to FortiClient (Linux) logs

Windows

This section contains the following information for FortiClient (Windows):

- [Mandatory fields on page 6](#): fields that are mandatory to all FortiClient (Windows) logs.
- [Log fields by type on page 7](#): fields that only apply to security event logs.
- [Log message by type on page 10](#): lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
vd	vdom	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
file	file location	string	256
virus	virus name	string	512
sigid	signature id	string	260
from	email from	string	128
to	email to	string	512
service	network protocol	string	64
vpn	vpn tunnel name	string	32
filesize	file size	int	20
checksum	file crc32 checksum	int	20
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
viruscat	virus category	string	260
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnseverity	severity level	string	8
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnref	reference of the vulnerability	string	256
vulnengine	engine version	string	64

Log Field Name	Description	Data Type	Length
vulnsignature	signature version	string	260
vulnproducts	name of the vulnerable product	string	2048
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32
devid	device ID	string	16
hostname	host name of local machine	string	256
pdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

systemevent

Log Field Name	Description	Data Type	Length
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
emshostname	EMS host name	string	64
status	status description	string	16
emsip	EMS IP	string	20
fctip	FCT IP	string	20
epmgmtst	management status	enumeration string	64
epquarmsg	quarant message	string	260
epfeatures	installed features list	string	128
epenfeatures	enabled features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32

Log Field Name	Description	Data Type	Length
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

Log message by type

securityevent > av

Log ID	Level	Sub Type	Event Type	Message																											
96530	warning	av	action	Found virus																											
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>action</td> <td>block or monitor</td> <td>string</td> </tr> <tr> <td>file</td> <td>file location</td> <td>string</td> </tr> <tr> <td>virus</td> <td>virus name</td> <td>string</td> </tr> <tr> <td>sigid</td> <td>signature id</td> <td>string</td> </tr> <tr> <td>from</td> <td>email from</td> <td>string</td> </tr> <tr> <td>to</td> <td>email to</td> <td>string</td> </tr> <tr> <td>service</td> <td>network protocol</td> <td>string</td> </tr> <tr> <td>vpn</td> <td>vpn tunnel name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	action	block or monitor	string	file	file location	string	virus	virus name	string	sigid	signature id	string	from	email from	string	to	email to	string	service	network protocol	string	vpn	vpn tunnel name	string
Field	Field Description	Field Type																													
action	block or monitor	string																													
file	file location	string																													
virus	virus name	string																													
sigid	signature id	string																													
from	email from	string																													
to	email to	string																													
service	network protocol	string																													
vpn	vpn tunnel name	string																													

Log ID	Level	Sub Type	Event Type	Message																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>filesize</td> <td>file size</td> <td>int</td> </tr> <tr> <td>checksum</td> <td>file crc32 checksum</td> <td>int</td> </tr> <tr> <td>detectedby</td> <td>the security feature that detected virus</td> <td>enumeration string</td> </tr> <tr> <td>detectedin</td> <td>where the virus is detected</td> <td>enumeration string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string															
Field	Field Description	Field Type																																
filesize	file size	int																																
checksum	file crc32 checksum	int																																
detectedby	the security feature that detected virus	enumeration string																																
detectedin	where the virus is detected	enumeration string																																
96531	warning	av	warning	Found malware																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>action</td> <td>block or monitor</td> <td>string</td> </tr> <tr> <td>file</td> <td>file location</td> <td>string</td> </tr> <tr> <td>virus</td> <td>virus name</td> <td>string</td> </tr> <tr> <td>viruscat</td> <td>virus category</td> <td>string</td> </tr> <tr> <td>sigid</td> <td>signature id</td> <td>string</td> </tr> <tr> <td>filesize</td> <td>file size</td> <td>int</td> </tr> <tr> <td>checksum</td> <td>file crc32 checksum</td> <td>int</td> </tr> <tr> <td>detectedby</td> <td>the security feature that detected virus</td> <td>enumeration string</td> </tr> <tr> <td>detectedin</td> <td>where the virus is detected</td> <td>enumeration string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	action	block or monitor	string	file	file location	string	virus	virus name	string	viruscat	virus category	string	sigid	signature id	string	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string
Field	Field Description	Field Type																																
action	block or monitor	string																																
file	file location	string																																
virus	virus name	string																																
viruscat	virus category	string																																
sigid	signature id	string																																
filesize	file size	int																																
checksum	file crc32 checksum	int																																
detectedby	the security feature that detected virus	enumeration string																																
detectedin	where the virus is detected	enumeration string																																

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message												
96521	info	vulnerabilityscan	status	A vulnerability scan result has been logged												
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulnid</td> <td>id of the vulnerability</td> <td>int</td> </tr> <tr> <td>vulnname</td> <td>name of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnseverity</td> <td>severity level</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulnid	id of the vulnerability	int	vulnname	name of the vulnerability	string	vulnseverity	severity level	string
Field	Field Description	Field Type														
vulnid	id of the vulnerability	int														
vulnname	name of the vulnerability	string														
vulnseverity	severity level	string														

Log ID	Level	Sub Type	Event Type	Message																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulncat</td> <td>category</td> <td>string</td> </tr> <tr> <td>vulncvss</td> <td>cvss score</td> <td>string</td> </tr> <tr> <td>vulnref</td> <td>reference of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnengine</td> <td>engine version</td> <td>string</td> </tr> <tr> <td>vulnsignature</td> <td>signature version</td> <td>string</td> </tr> <tr> <td>vulnproducts</td> <td>name of the vulnerable product</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulncat	category	string	vulncvss	cvss score	string	vulnref	reference of the vulnerability	string	vulnengine	engine version	string	vulnsignature	signature version	string	vulnproducts	name of the vulnerable product	string									
Field	Field Description	Field Type																																
vulncat	category	string																																
vulncvss	cvss score	string																																
vulnref	reference of the vulnerability	string																																
vulnengine	engine version	string																																
vulnsignature	signature version	string																																
vulnproducts	name of the vulnerable product	string																																
96522	info	vulnerabilityscan	status	Applying patch for vulnerability found																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulnid</td> <td>id of the vulnerability</td> <td>int</td> </tr> <tr> <td>vulnname</td> <td>name of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnseverity</td> <td>severity level</td> <td>string</td> </tr> <tr> <td>vulncat</td> <td>category</td> <td>string</td> </tr> <tr> <td>vulncvss</td> <td>cvss score</td> <td>string</td> </tr> <tr> <td>vulnref</td> <td>reference of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnengine</td> <td>engine version</td> <td>string</td> </tr> <tr> <td>vulnsignature</td> <td>signature version</td> <td>string</td> </tr> <tr> <td>vulnproducts</td> <td>name of the vulnerable product</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulnid	id of the vulnerability	int	vulnname	name of the vulnerability	string	vulnseverity	severity level	string	vulncat	category	string	vulncvss	cvss score	string	vulnref	reference of the vulnerability	string	vulnengine	engine version	string	vulnsignature	signature version	string	vulnproducts	name of the vulnerable product	string
Field	Field Description	Field Type																																
vulnid	id of the vulnerability	int																																
vulnname	name of the vulnerability	string																																
vulnseverity	severity level	string																																
vulncat	category	string																																
vulncvss	cvss score	string																																
vulnref	reference of the vulnerability	string																																
vulnengine	engine version	string																																
vulnsignature	signature version	string																																
vulnproducts	name of the vulnerable product	string																																

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message
96953	info	endpoint	status	Endpoint Control Status Changed

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>eponlinest</td> <td>online status</td> <td>enumeration string</td> </tr> <tr> <td>epplace</td> <td>EP place</td> <td>enumeration string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> <tr> <td>status</td> <td>status description</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	eponlinest	online status	enumeration string	epplace	EP place	enumeration string	emshostname	EMS host name	string	status	status description	string			
Field	Field Description	Field Type																				
eponlinest	online status	enumeration string																				
epplace	EP place	enumeration string																				
emshostname	EMS host name	string																				
status	status description	string																				
96955	info	endpoint	status	Endpoint Control Registration Status Changed																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> <tr> <td>status</td> <td>status description</td> <td>string</td> </tr> <tr> <td>emsip</td> <td>EMS IP</td> <td>string</td> </tr> <tr> <td>fctip</td> <td>FCT IP</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	emshostname	EMS host name	string	status	status description	string	emsip	EMS IP	string	fctip	FCT IP	string			
Field	Field Description	Field Type																				
emshostname	EMS host name	string																				
status	status description	string																				
emsip	EMS IP	string																				
fctip	FCT IP	string																				
96956	info	endpoint	status	Endpoint Quarantine Status Changed																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>epmgmtst</td> <td>management status</td> <td>enumeration string</td> </tr> <tr> <td>epquarmsg</td> <td>quarant message</td> <td>string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	epmgmtst	management status	enumeration string	epquarmsg	quarant message	string	emshostname	EMS host name	string						
Field	Field Description	Field Type																				
epmgmtst	management status	enumeration string																				
epquarmsg	quarant message	string																				
emshostname	EMS host name	string																				
96957	info	endpoint	status	Endpoint Ext Log to FAZ																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>epfeatures</td> <td>installed features list</td> <td>string</td> </tr> <tr> <td>openfeatures</td> <td>enabled features list</td> <td>string</td> </tr> <tr> <td>ephbemsduration</td> <td>EMS heart beat duration</td> <td>int</td> </tr> <tr> <td>ephbemslast</td> <td>EMS heart beat last time</td> <td>string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	epfeatures	installed features list	string	openfeatures	enabled features list	string	ephbemsduration	EMS heart beat duration	int	ephbemslast	EMS heart beat last time	string	emshostname	EMS host name	string
Field	Field Description	Field Type																				
epfeatures	installed features list	string																				
openfeatures	enabled features list	string																				
ephbemsduration	EMS heart beat duration	int																				
ephbemslast	EMS heart beat last time	string																				
emshostname	EMS host name	string																				
96958	info	endpoint	status	User social media information																		

Log ID	Level	Sub Type	Event Type	Message															
				<table><thead><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr></thead><tbody><tr><td>social_email</td><td>social email</td><td>string</td></tr><tr><td>social_phone</td><td>social phone number</td><td>string</td></tr><tr><td>social_srvc</td><td>social service</td><td>string</td></tr><tr><td>social_user</td><td>social user name</td><td>string</td></tr></tbody></table>	Field	Field Description	Field Type	social_email	social email	string	social_phone	social phone number	string	social_srvc	social service	string	social_user	social user name	string
Field	Field Description	Field Type																	
social_email	social email	string																	
social_phone	social phone number	string																	
social_srvc	social service	string																	
social_user	social user name	string																	

Linux

This section contains the following information for FortiClient (Linux):

- [Mandatory fields on page 15](#): fields that are mandatory to all FortiClient (Linux) logs.
- [Log fields by type on page 16](#): fields that only apply to security event logs.
- [Log message by type on page 19](#): lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
vd	vdom	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
file	file location	string	256
virus	virus name	string	512
sigid	signature id	string	260
from	email from	string	128
to	email to	string	512
service	network protocol	string	64
vpn	vpn tunnel name	string	32
filesize	file size	int	20
checksum	file crc32 checksum	int	20
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
viruscat	virus category	string	260
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnseverity	severity level	string	8
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnref	reference of the vulnerability	string	256
vulnengine	engine version	string	64

Log Field Name	Description	Data Type	Length
vulnsignature	signature version	string	260
vulnproducts	name of the vulnerable product	string	2048
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

systemevent

Log Field Name	Description	Data Type	Length
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
emshostname	EMS host name	string	64
status	status description	string	16
emsip	EMS IP	string	20
fctip	FCT IP	string	20
epgmtst	management status	enumeration string	64
epquarmsg	quarant message	string	260
epfeatures	installed features list	string	128
epenfeatures	enabled features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32

Log Field Name	Description	Data Type	Length
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

Log message by type

securityevent > av

Log ID	Level	Sub Type	Event Type	Message																											
96530	warning	av	action	Found virus																											
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>action</td> <td>block or monitor</td> <td>string</td> </tr> <tr> <td>file</td> <td>file location</td> <td>string</td> </tr> <tr> <td>virus</td> <td>virus name</td> <td>string</td> </tr> <tr> <td>sigid</td> <td>signature id</td> <td>string</td> </tr> <tr> <td>from</td> <td>email from</td> <td>string</td> </tr> <tr> <td>to</td> <td>email to</td> <td>string</td> </tr> <tr> <td>service</td> <td>network protocol</td> <td>string</td> </tr> <tr> <td>vpn</td> <td>vpn tunnel name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	action	block or monitor	string	file	file location	string	virus	virus name	string	sigid	signature id	string	from	email from	string	to	email to	string	service	network protocol	string	vpn	vpn tunnel name	string
Field	Field Description	Field Type																													
action	block or monitor	string																													
file	file location	string																													
virus	virus name	string																													
sigid	signature id	string																													
from	email from	string																													
to	email to	string																													
service	network protocol	string																													
vpn	vpn tunnel name	string																													

Log ID	Level	Sub Type	Event Type	Message																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>filesize</td> <td>file size</td> <td>int</td> </tr> <tr> <td>checksum</td> <td>file crc32 checksum</td> <td>int</td> </tr> <tr> <td>detectedby</td> <td>the security feature that detected virus</td> <td>enumeration string</td> </tr> <tr> <td>detectedin</td> <td>where the virus is detected</td> <td>enumeration string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string															
Field	Field Description	Field Type																																
filesize	file size	int																																
checksum	file crc32 checksum	int																																
detectedby	the security feature that detected virus	enumeration string																																
detectedin	where the virus is detected	enumeration string																																
96531	warning	av	warning	Found malware																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>action</td> <td>block or monitor</td> <td>string</td> </tr> <tr> <td>file</td> <td>file location</td> <td>string</td> </tr> <tr> <td>virus</td> <td>virus name</td> <td>string</td> </tr> <tr> <td>viruscat</td> <td>virus category</td> <td>string</td> </tr> <tr> <td>sigid</td> <td>signature id</td> <td>string</td> </tr> <tr> <td>filesize</td> <td>file size</td> <td>int</td> </tr> <tr> <td>checksum</td> <td>file crc32 checksum</td> <td>int</td> </tr> <tr> <td>detectedby</td> <td>the security feature that detected virus</td> <td>enumeration string</td> </tr> <tr> <td>detectedin</td> <td>where the virus is detected</td> <td>enumeration string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	action	block or monitor	string	file	file location	string	virus	virus name	string	viruscat	virus category	string	sigid	signature id	string	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string
Field	Field Description	Field Type																																
action	block or monitor	string																																
file	file location	string																																
virus	virus name	string																																
viruscat	virus category	string																																
sigid	signature id	string																																
filesize	file size	int																																
checksum	file crc32 checksum	int																																
detectedby	the security feature that detected virus	enumeration string																																
detectedin	where the virus is detected	enumeration string																																

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message												
96521	info	vulnerabilityscan	status	A vulnerability scan result has been logged												
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulnid</td> <td>id of the vulnerability</td> <td>int</td> </tr> <tr> <td>vulnname</td> <td>name of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnseverity</td> <td>severity level</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulnid	id of the vulnerability	int	vulnname	name of the vulnerability	string	vulnseverity	severity level	string
Field	Field Description	Field Type														
vulnid	id of the vulnerability	int														
vulnname	name of the vulnerability	string														
vulnseverity	severity level	string														

Log ID	Level	Sub Type	Event Type	Message																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulncat</td> <td>category</td> <td>string</td> </tr> <tr> <td>vulncvss</td> <td>cvss score</td> <td>string</td> </tr> <tr> <td>vulnref</td> <td>reference of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnengine</td> <td>engine version</td> <td>string</td> </tr> <tr> <td>vulnsignature</td> <td>signature version</td> <td>string</td> </tr> <tr> <td>vulnproducts</td> <td>name of the vulnerable product</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulncat	category	string	vulncvss	cvss score	string	vulnref	reference of the vulnerability	string	vulnengine	engine version	string	vulnsignature	signature version	string	vulnproducts	name of the vulnerable product	string									
Field	Field Description	Field Type																																
vulncat	category	string																																
vulncvss	cvss score	string																																
vulnref	reference of the vulnerability	string																																
vulnengine	engine version	string																																
vulnsignature	signature version	string																																
vulnproducts	name of the vulnerable product	string																																
96522	info	vulnerabilityscan	status	Applying patch for vulnerability found																														
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>vulnid</td> <td>id of the vulnerability</td> <td>int</td> </tr> <tr> <td>vulnname</td> <td>name of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnseverity</td> <td>severity level</td> <td>string</td> </tr> <tr> <td>vulncat</td> <td>category</td> <td>string</td> </tr> <tr> <td>vulncvss</td> <td>cvss score</td> <td>string</td> </tr> <tr> <td>vulnref</td> <td>reference of the vulnerability</td> <td>string</td> </tr> <tr> <td>vulnengine</td> <td>engine version</td> <td>string</td> </tr> <tr> <td>vulnsignature</td> <td>signature version</td> <td>string</td> </tr> <tr> <td>vulnproducts</td> <td>name of the vulnerable product</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	vulnid	id of the vulnerability	int	vulnname	name of the vulnerability	string	vulnseverity	severity level	string	vulncat	category	string	vulncvss	cvss score	string	vulnref	reference of the vulnerability	string	vulnengine	engine version	string	vulnsignature	signature version	string	vulnproducts	name of the vulnerable product	string
Field	Field Description	Field Type																																
vulnid	id of the vulnerability	int																																
vulnname	name of the vulnerability	string																																
vulnseverity	severity level	string																																
vulncat	category	string																																
vulncvss	cvss score	string																																
vulnref	reference of the vulnerability	string																																
vulnengine	engine version	string																																
vulnsignature	signature version	string																																
vulnproducts	name of the vulnerable product	string																																

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message
96953	info	endpoint	status	Endpoint Control Status Changed

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>eponlinest</td> <td>online status</td> <td>enumeration string</td> </tr> <tr> <td>epplace</td> <td>EP place</td> <td>enumeration string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> <tr> <td>status</td> <td>status description</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	eponlinest	online status	enumeration string	epplace	EP place	enumeration string	emshostname	EMS host name	string	status	status description	string			
Field	Field Description	Field Type																				
eponlinest	online status	enumeration string																				
epplace	EP place	enumeration string																				
emshostname	EMS host name	string																				
status	status description	string																				
96955	info	endpoint	status	Endpoint Control Registration Status Changed																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> <tr> <td>status</td> <td>status description</td> <td>string</td> </tr> <tr> <td>emsip</td> <td>EMS IP</td> <td>string</td> </tr> <tr> <td>fctip</td> <td>FCT IP</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	emshostname	EMS host name	string	status	status description	string	emsip	EMS IP	string	fctip	FCT IP	string			
Field	Field Description	Field Type																				
emshostname	EMS host name	string																				
status	status description	string																				
emsip	EMS IP	string																				
fctip	FCT IP	string																				
96956	info	endpoint	status	Endpoint Quarantine Status Changed																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>epgmtst</td> <td>management status</td> <td>enumeration string</td> </tr> <tr> <td>epquarmsg</td> <td>quarant message</td> <td>string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	epgmtst	management status	enumeration string	epquarmsg	quarant message	string	emshostname	EMS host name	string						
Field	Field Description	Field Type																				
epgmtst	management status	enumeration string																				
epquarmsg	quarant message	string																				
emshostname	EMS host name	string																				
96957	info	endpoint	status	Endpoint Ext Log to FAZ																		
				<table border="1"> <thead> <tr> <th>Field</th> <th>Field Description</th> <th>Field Type</th> </tr> </thead> <tbody> <tr> <td>epfeatures</td> <td>installed features list</td> <td>string</td> </tr> <tr> <td>openfeatures</td> <td>enabled features list</td> <td>string</td> </tr> <tr> <td>epbemsduration</td> <td>EMS heart beat duration</td> <td>int</td> </tr> <tr> <td>epbemslast</td> <td>EMS heart beat last time</td> <td>string</td> </tr> <tr> <td>emshostname</td> <td>EMS host name</td> <td>string</td> </tr> </tbody> </table>	Field	Field Description	Field Type	epfeatures	installed features list	string	openfeatures	enabled features list	string	epbemsduration	EMS heart beat duration	int	epbemslast	EMS heart beat last time	string	emshostname	EMS host name	string
Field	Field Description	Field Type																				
epfeatures	installed features list	string																				
openfeatures	enabled features list	string																				
epbemsduration	EMS heart beat duration	int																				
epbemslast	EMS heart beat last time	string																				
emshostname	EMS host name	string																				
96958	info	endpoint	status	User social media information																		

Log ID	Level	Sub Type	Event Type	Message															
				<table><thead><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr></thead><tbody><tr><td>social_email</td><td>social email</td><td>string</td></tr><tr><td>social_phone</td><td>social phone number</td><td>string</td></tr><tr><td>social_srvc</td><td>social service</td><td>string</td></tr><tr><td>social_user</td><td>social user name</td><td>string</td></tr></tbody></table>	Field	Field Description	Field Type	social_email	social email	string	social_phone	social phone number	string	social_srvc	social service	string	social_user	social user name	string
Field	Field Description	Field Type																	
social_email	social email	string																	
social_phone	social phone number	string																	
social_srvc	social service	string																	
social_user	social user name	string																	



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.